

NON-VANISHING THEOREMS FOR QUADRATIC TWISTS OF ELLIPTIC CURVES

SHUAI ZHAI

CONTENTS

1. Introduction	1
2. Modular symbols	5
3. Period lattice and the proof of non-vanishing results	8
4. Quadratic twists of Neumann-Setzer elliptic curves	10
4.1. Classical 2-descents	11
4.2. Behaviour of Hecke eigenvalues	16
4.3. 2-part of Birch and Swinnerton-Dyer conjecture	17
References	18

1. INTRODUCTION

Let E be an elliptic curve defined over \mathbb{Q} , and let $L(E, s)$ be the complex L -series of E . For each square free non-zero integer $d \neq 1$, we write $E^{(d)}$ for the twist of E by the quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, and $L(E^{(d)}, s)$ for its complex L -series. Let C_E , or simply C when there is no danger of confusion, denote the conductor of E . As usual, $\Gamma_0(C)$ will denote the subgroup of $SL_2(\mathbb{Z})$ consisting of all matrices with the bottom left hand corner entry divisible by C , and we write $X_0(C)$ for the corresponding modular curve. It is known that, by the theorem of Wiles [17], Taylor-Wiles [13] and Breuil-Conrad-Diamond-Taylor [2], all elliptic curves E/\mathbb{Q} have a modular parametrization, i.e. there is a non-constant map φ from the modular curve $X_0(C)$ to E such that the pull-back of a holomorphic differential on E is a modular form (newform) of weight 2 and level C , and the integer C being the conductor of E . An elliptic curve over \mathbb{Q} is optimal if it is an optimal quotient of the corresponding modular curve. Every isogeny class contains a unique optimal curve. The optimal curve has minimal degree in the isogeny class. We denote the modular degree of E to be $\deg(\varphi)$. Zagier [18] gave an algorithm to compute $\deg(\varphi)$ when the conductor C is a prime. Cremona [6] generalised Zagier's method and derived an explicit formula for $\deg(\varphi)$ for arbitrary C , in terms of modular symbols.

Let \mathcal{H} be the upper half plane, denote $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}_1(\mathbb{Q})$. Let Λ_f be the period lattice of the newform $f \in S_2(\Gamma_0(C))$. Since the differential $f(z)dz$ is holomorphic, the function $I_f(z_0) = 2\pi i \int_{z_0}^{\infty} f(z)dz$ is well-defined for $z_0 \in \mathcal{H}^*$ and independent of the path from z_0 to ∞ . For $g \in \Gamma_0(C)$, the function $P_f(g) = I_f(z_0) - I_f(g(z_0)) = 2\pi i \int_{z_0}^{g(z_0)} f(z)dz$ is independent of z_0 , and defines a group homomorphism $P_f : \Gamma_0(C) \rightarrow \mathbb{C}$. If the image of P_f is contained in the lattice Λ_f , then the map I_f induces a map

$$\begin{aligned} \varphi : \Gamma_0(C) \backslash \mathcal{H}^* &\rightarrow E = \mathbb{C}/\Lambda_f \\ z \bmod \Gamma_0(C) &\mapsto I_f(z) \bmod \Lambda_f. \end{aligned}$$

Moreover, by the theorem of Manin-Drinfeld, we know that $\varphi([0])$ is a torsion point on E , which is defined over \mathbb{Q} . For each square free integer M , prime to C , with $M \equiv 1 \pmod{4}$, we define

$$L^{(alg)}(E^{(M)}, 1) = L(E^{(M)}, 1)/\Omega_{\infty}(E^{(M)}),$$

which is well known to be a rational number, where $\Omega_{\infty}(E^{(M)})$ is the least real period of $E^{(M)}$. We will always normalise the order valuation at 2 by $\text{ord}_2(2) = 1$. Let $F(x)$ be the 2-division polynomial of E . When $F(x)$ is irreducible over \mathbb{Q} , we define F to be the field obtained by adjoining to \mathbb{Q} one fixed root of $F(x)$. Let q be any prime of good reduction for E , and let a_q be the trace of Frobenius at q on E and denote $N_q := 1 + q - a_q$. For each integer $m > 1$, let $E[m]$ denote the group of m -division points on E . Also, we define a rational prime q to be inert in the field F if it is unramified and there is a unique

prime of F above q . By applying some results by Manin [9] and Cremona [5] on modular symbols, we prove the following general results.

We first give results for curves E with $E[2](\mathbb{Q}) = 0$.

Theorem 1.1. *Let E be a $\Gamma_0(C)$ -optimal elliptic curve over \mathbb{Q} , with negative discriminant, with $E[2](\mathbb{Q}) = 0$, and satisfying $\text{ord}_2(L^{(alg)}(E, 1)) = 0$. Let M be any integer of the form $M = \epsilon q_1 q_2 \cdots q_r$, where $r \geq 1$, q_1, \dots, q_r are arbitrary distinct odd primes which are inert in the field F , and the sign $\epsilon = \pm 1$ is chosen so that $M \equiv 1 \pmod{4}$. Then we have*

$$\text{ord}_2(L^{(alg)}(E^{(M)}, 1)) = 0.$$

In particular, $L(E^{(M)}, s)$ does not vanish at $s = 1$, and so $E^{(M)}(\mathbb{Q})$ and $\text{III}(E^{(M)}(\mathbb{Q}))$ are finite.

We remark here that, by the above theorem and the work of Boxer and Diao [1, Theorem 1.2], the 2-part of Birch and Swinnerton-Dyer conjecture is valid for $L(E^{(M)}, s)$, with $M = \epsilon q_1 q_2 \cdots q_r \equiv 1 \pmod{4}$, where $r \geq 1$, q_1, \dots, q_r are arbitrary distinct odd primes which are inert in the field F , and E is an elliptic curve satisfying the conditions in Theorem 1.1 and the following further conditions: 1) The 2-Selmer rank of E is 0; 2) If p is any prime for which E has bad reduction, then E has multiplicative reduction at p and the p -adic valuation of the discriminant of E is odd; 3) E has good reduction at 2 and the reduction of $E \pmod{2}$ has j -invariant 0.

Of course, the Chebotarev theorem shows that there is a positive density of primes which are inert in F . Here are some examples of curves to which Theorem 1.1 applies, such as $X_0(11)$, which we view as an elliptic curve by taking $[\infty]$ to be the origin of the group law, and which has a minimal Weierstrass equation given by

$$E : y^2 + y = x^3 - x^2 - 10x - 20.$$

Moreover, $E(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$, $L^{(alg)}(E, 1) = \frac{1}{5}$, and it has discriminant -11^5 . A simple form of the 2-division polynomial is $F(x) = x^3 - x^2 + x + 1$, which has discriminant -44 . Here are a list of odd primes which are inert in the field F :

$$3, 5, 23, 31, 37, 59, 67, 71, 89, 97, 113, 137, 157, 179, 181, 191, \dots$$

The 2-part of Birch and Swinnerton-Dyer conjecture is valid for all these twists. Further examples of elliptic curves E to which Theorem 1.1 applies are as follows (we use Cremona's label for each curve). First we can take $E = X_0(19)$, which has conductor 19 and equation

$$19A1 : y^2 + y = x^3 + x^2 - 9x - 15,$$

also we can take the curves

$$26A1 : y^2 + xy + y = x^3 - 5x - 8, \text{ and } 26B1 : y^2 + xy + y = x^3 - x^2 - 3x + 3,$$

which have conductor 26, and the curves

$$121A1 : y^2 + xy + y = x^3 + x^2 - 30x - 76, \text{ and } 121C1 : y^2 + xy = x^3 + x^2 - 2x - 7,$$

which have conductor 121.

When E has positive discriminant, an entirely parallel result holds, provided we only consider twists by $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$ with $M > 0$, and $M \equiv 1 \pmod{4}$.

Theorem 1.2. *Let E be a $\Gamma_0(C)$ -optimal elliptic curve over \mathbb{Q} , with positive discriminant, with $E[2](\mathbb{Q}) = 0$, and satisfying $\text{ord}_2(L^{(alg)}(E, 1)) = 1$. Let M be any positive integer of the form $M = q_1 q_2 \cdots q_r$, where $r \geq 1$, q_1, \dots, q_r are arbitrary distinct odd primes which are inert in the field F , and $M \equiv 1 \pmod{4}$. Then we have*

$$\text{ord}_2(L^{(alg)}(E^{(M)}, 1)) = 1.$$

In particular, $L(E^{(M)}, s)$ does not vanish at $s = 1$, and so $E^{(M)}(\mathbb{Q})$ and $\text{III}(E^{(M)}(\mathbb{Q}))$ are finite.

Here are some examples of curves to which Theorem 1.2 applies, such as $E = 37B1$, which has a minimal Weierstrass equation given by

$$E : y^2 + y = x^3 + x^2 - 23x - 50.$$

Moreover, $E(\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$, $L^{(alg)}(E, 1) = \frac{2}{3}$, and it has discriminant 37^3 . A simple form of the 2-division polynomial is $F(x) = x^3 + x^2 - 3x - 1$, which has discriminant 148. Here are a list of odd primes which are inert in the field F :

$$3, 7, 11, 41, 47, 53, 71, 73, 83, 101, 127, 149, 157, 173, 181, 197, \dots$$

Further examples of elliptic curves E to which Theorem 1.2 applies are as follows. First we can take 141E1, which has conductor 141 and equation

$$141E1 : y^2 + y = x^3 + x^2 - 26x - 61,$$

also we can take the curves

$$142D1 : y^2 + xy = x^3 - 8x + 8, \text{ and } 142E1 : y^2 + xy = x^3 - x^2 - 2626x + 52244,$$

which have conductor 142.

It is not difficult to see that Theorems 1.1 and 1.2 are entirely consistent with the 2-part of the conjecture of Birch and Swinnerton-Dyer, provided we know the non-vanishing of the L -series of the relevant twists of E at $s = 1$, and that the 2-primary subgroup of the Tate-Shafarevich group of the relevant twists is zero (see the discussion at the end of Section 2). However, we remark that it is not straightforward to carry out a classical 2-descent on these curves because of our hypothesis that $E[2](\mathbb{Q}) = 0$.

For curves E with $E[2](\mathbb{Q}) \neq 0$, we have only been able to establish the following much weaker results in which we only consider twists by $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$ with $M \equiv 1 \pmod{4}$ and divisible by only one prime.

Theorem 1.3. *Let E be a $\Gamma_0(C)$ -optimal elliptic curve over \mathbb{Q} , with negative discriminant. Let M be any integer of the form $M = \epsilon q$, where q is an arbitrary odd prime, and the sign $\epsilon = \pm 1$ is chosen so that $M \equiv 1 \pmod{4}$. Assume $L(E, 1) \neq 0$. If $\text{ord}_2(N_q) = -\text{ord}_2(L^{(\text{alg})}(E, 1)) \neq 0$, then we have*

$$\text{ord}_2(L^{(\text{alg})}(E^{(M)}, 1)) = 0.$$

In particular, $L(E^{(M)}, s)$ does not vanish at $s = 1$, and so $E^{(M)}(\mathbb{Q})$ and $\text{III}(E^{(M)}(\mathbb{Q}))$ are finite.

Note that, in the above theorem, we are assuming, in particular, that $\text{ord}_2(L^{(\text{alg})}(E, 1)) < 0$. It is not known at present how to deduce from this assumption that $E[2](\mathbb{Q})$ is non-zero, although of course this would follow from the conjecture of Birch and Swinnerton-Dyer for E . Here are some examples of curves to which Theorem 1.3 applies, such as the Neumann-Setzer elliptic curves, which have conductor p , where p is a prime of the form $u^2 + 64$ for some integer $u \equiv 1 \pmod{4}$, which have a minimal Weierstrass equation given by

$$A : y^2 + xy = x^3 + \frac{u-1}{4}x^2 + 4x + u.$$

We shall consider all these curves in details and prove the following theorem in Section 4.

Theorem 1.4. *Let q be any prime congruent to 3 modulo 4 and inert in $\mathbb{Q}(\sqrt{p})$. When $u \equiv 5 \pmod{8}$, we have that*

$$\text{ord}_2(L^{(\text{alg})}(A^{(-q)}, 1)) = 0.$$

In particular, $L(A^{(-q)}, s)$ does not vanish at $s = 1$, and so $A^{(-q)}(\mathbb{Q})$ is finite, the Tate-Shafarevich group $\text{III}(A^{(-q)}(\mathbb{Q}))$ is finite of odd cardinality, and the 2-part of Birch and Swinnerton-Dyer conjecture is valid for $A^{(-q)}$.

Here we take $X_0(17)$ as another example, which has a minimal Weierstrass equation given by

$$E : y^2 + xy + y = x^3 - x^2 - x - 14.$$

Moreover, $E(\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$, $L^{(\text{alg})}(E, 1) = \frac{1}{4}$, and it has discriminant -17^4 . In particular, our theorem applies to all primes q with $q \equiv 3 \pmod{4}$ and which are inert in $\mathbb{Q}(\sqrt{17})$, whence $N_q \equiv 4 \pmod{8}$. Here are a list of odd primes satisfying the above conditions:

$$3, 7, 11, 23, 31, 71, 79, 107, 131, 139, 163, 167, 199, \dots$$

The Chebotarev theorem shows that there is a positive density of primes which are both inert in $\mathbb{Q}(\sqrt{i})$ and $\mathbb{Q}(\sqrt{17})$. For the twists $E^{(-q)}$ for such primes q , it is easy to show by a classical 2-descent that $E^{(-q)}(\mathbb{Q})$ is finite and that $\text{III}(E^{(-q)}(\mathbb{Q}))[2] = 0$. Thus the 2-part of the Birch-Swinnerton-Dyer conjecture is valid for $E^{(-q)}$. Further examples of elliptic curves E to which Theorem 1.3 applies are as follows. First we can take $E = X_0(14)$, which has conductor 14 and equation

$$14A1 : y^2 + xy + y = x^3 + 4x - 6,$$

also we can take the curve $X_0(49)$, which has conductor 49 and equation

$$49A1 : y^2 + xy = x^3 - x^2 - 2x - 1,$$

and which has been fully investigated by Coates, Li, Tian, and Zhai by Zhao's method and Waldspurger's formula (see [3]).

Similarly, when E has positive discriminant, an entirely parallel result holds, provided we only consider twists by $\mathbb{Q}(\sqrt{q})/\mathbb{Q}$ with some prime $q \equiv 1 \pmod{4}$.

Theorem 1.5. *Let E be a $\Gamma_0(C)$ -optimal elliptic curve over \mathbb{Q} , with positive discriminant. Let q be any odd prime with $q \equiv 1 \pmod{4}$. Assume $L(E, 1) \neq 0$. If $\text{ord}_2(N_q) = 1 - \text{ord}_2(L^{(alg)}(E, 1)) \neq 0$, then we have*

$$\text{ord}_2(L^{(alg)}(E^{(q)}, 1)) = 1.$$

In particular, $L(E^{(q)}, s)$ does not vanish at $s = 1$, and so $E^{(q)}(\mathbb{Q})$ and $\text{III}(E^{(q)}(\mathbb{Q}))$ are finite.

Here are some examples of curves to which Theorem 1.5 applies, such as $X_0(21)$, which has a minimal Weierstrass equation given by

$$E : y^2 + xy = x^3 - 4x - 1.$$

Moreover, $E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $L^{(alg)}(E, 1) = \frac{1}{4}$, and it has discriminant $3^4 \cdot 7^2$. In particular, our theorem applies to all primes q with $q \equiv 1 \pmod{4}$ and which are both inert in $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{7})$, whence $N_q \equiv 8 \pmod{16}$. Here are a list of odd primes satisfying the above conditions:

$$5, 17, 41, 89, 101, 173, 269, 293, \dots$$

The Chebotarev theorem shows that there is a positive density of primes congruent to 1 modulo 4 which are both inert in $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{7})$. For the twists $E^{(q)}$ for such primes q , it is easy to show that $E^{(q)}(\mathbb{Q})$ is finite and that $\text{III}(E^{(q)}(\mathbb{Q}))[2] = 0$. Thus the 2-part of the Birch-Swinnerton-Dyer conjecture is valid for $E^{(q)}$. Further examples of elliptic curves E to which Theorem 1.5 applies are as follows. First we can take $E = X_0(33)$, which has conductor 33 and equation

$$33A1 : y^2 + xy = x^3 + x^2 - 11x,$$

also we can take $E = X_0(34)$, which has conductor 34 and equation

$$34A1 : y^2 + xy = x^3 - 3x + 1.$$

It is not difficult to see that Theorems 1.3 and 1.5 are also entirely consistent with the 2-part of the conjecture of Birch and Swinnerton-Dyer. Moreover, it is easy to carry out a straightforward classical 2-descent on these curves because of our hypothesis that $E[2](\mathbb{Q}) \neq 0$. Then after considering the behaviour of Tamagawa factors under twisting (see the lemma at the end of Section 2), one can verify the 2-part of Birch and Swinnerton-Dyer conjecture for all these curves.

For curves E with $\text{ord}_2(L^{(alg)}(E, 1)) \neq 0$ and negative discriminant, we could obtain the following lower bound for some twists of E .

Theorem 1.6. *Let E be a $\Gamma_0(C)$ -optimal elliptic curve over \mathbb{Q} , with negative discriminant, and satisfying $L(E, 1) \neq 0$. Let M be any integer of the form $M = \epsilon q_1 q_2 \cdots q_r$, where $r \geq 1$, q_1, \dots, q_r are arbitrary distinct odd primes, and the sign $\epsilon = \pm 1$ is chosen so that $M \equiv 1 \pmod{4}$. If $\text{ord}_2(N_{q_i}) > -\text{ord}_2(L^{(alg)}(E, 1))$ holds for at least one prime factor q_i ($1 \leq i \leq r$) of M , then we have*

$$\text{ord}_2(L^{(alg)}(E^{(M)}, 1)) \geq 1.$$

We remark that Theorem 1.6 can apply to all the $\Gamma_0(C)$ -optimal elliptic curves with negative discriminant, and satisfying $L(E, 1) \neq 0$. When E has positive discriminant, we have the following trivial lower bound result.

Theorem 1.7. *Let E be a $\Gamma_0(C)$ -optimal elliptic curve over \mathbb{Q} , with positive discriminant, and satisfying $L(E, 1) \neq 0$. Let $M \neq 1$ be any integer with $M \equiv 1 \pmod{4}$, then we have*

$$\text{ord}_2(L^{(alg)}(E^{(M)}, 1)) \geq 1.$$

We remark that the integer $\text{ord}_2(L^{(alg)}(E, 1)) + \text{ord}_2(N_q)$ could not be negative by an easy observation of Manin's modular symbol formula, which will be talked about in the following section.

In conclusion, I am extremely grateful to my supervisor John Coates, and to John Cremona for his very helpful remarks on the questions discussed in this paper. I also would like to thank China Scholarship Council for supporting me studying in the Department of Pure Mathematics and Mathematical Statistics, University of Cambridge.

2. MODULAR SYMBOLS

Modular symbols were first introduced by Birch and Manin [9] several decades ago and since then have been studied, refined, and reformulated by several authors. They provide an explicit description of classical modular forms by a finite set of algebraic integers, and thus are the main tool for computations of modular forms. In this section, we are focusing on the modular forms in the space $S_2(\Gamma_0(C))$, which is closely corresponding to elliptic curves and could be computed in terms of modular symbols.

Let \mathcal{H} be the upper half plane, denote $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}_1(\mathbb{Q})$. Let $g \in G = \Gamma_0(C)$. Let α, β be two points in \mathcal{H}^* such that $\beta = g\alpha$. Then any path from α to β on \mathcal{H}^* is a closed path on $X_0(C)$ whose homology class only depends on α and β . Hence it determines an integral homology class in $H_1(X_0(C), \mathbb{Z})$, and we denote this homology class by the *modular symbol* $\{\alpha, \beta\}_G \in H_1(X_0(C), \mathbb{Z})$, or simple $\{\alpha, \beta\}$ when the group G is clear.

Let $\alpha, \beta, \gamma \in \mathcal{H}^*$ and $g, g_1, g_2 \in G$. The following properties could be obtained easily by the definition and one can find a proof in [5, Chapter 2] and [9]:

- 1) $\{\alpha, \alpha\} = 0$;
- 2) $\{\alpha, \beta\} + \{\beta, \alpha\} = 0$;
- 3) $\{\alpha, \beta\} + \{\beta, \gamma\} + \{\gamma, \alpha\} = 0$;
- 4) $\{g\alpha, g\beta\}_G = \{\alpha, \beta\}_G$;
- 5) $\{\alpha, g\alpha\}_G = \{\beta, g\beta\}_G$;
- 6) $\{\alpha, g_1 g_2 \alpha\}_G = \{\alpha, g_1 \alpha\}_G + \{\alpha, g_2 \alpha\}_G$;
- 7) $\{\alpha, g\alpha\}_G \in H_1(X_0(C), \mathbb{Z})$.

The following theorem, which were proved by Manin [9] and Drinfeld, stated that the difference of two cusps of a modular curve has finite order in the Jacobian variety.

Theorem 2.1. (*Manin-Drinfeld*) *Let G be a congruence subgroup of the modular group Γ , then for all pairs of cusps $\alpha, \beta \in \mathcal{H}^*$, we have*

$$\{\alpha, \beta\}_G \in H_1(X_0(C), \mathbb{Q}).$$

Moreover, Manin [9] gave some explicit formulae in terms of modular symbols to compute the central values of the L -functions attached to elliptic curves.

We now denote $\langle \{\alpha, \beta\}, f \rangle := \int_{\alpha}^{\beta} 2\pi i f(z) dz$. Let m be a positive integer satisfying $(m, C) = 1$. According to Birch, Manin [9, Theorem 4.2] and Cremona [5, Chapter 3], we have the following two modular symbols formulae:

$$(2.1) \quad \left(\sum_{l|m} l - a_m \right) L(f, 1) = - \sum_{\substack{l|m \\ k \bmod l}} \langle \{0, \frac{k}{l}\}, f \rangle,$$

where l runs over all positive divisors of m , and

$$(2.2) \quad L(f, \chi, 1) = \frac{g(\chi)}{m} \sum_{k \bmod m} \bar{\chi}(k) \langle \{0, \frac{k}{m}\}, f \rangle,$$

where χ is a primitive character modulo m , and $g(\chi)$ is the Gauss sum $\sum_{k \bmod m} \chi(k) e^{2\pi i \frac{k}{m}}$. These two formulae are playing an important role in the proof of our results.

We now let Ω^+ ($i\Omega^-$) denote the least positive real (imaginary) period of the Neron differential of a global minimal equation for E . For each odd square free positive integer m , we define $r(m)$ to be the number of prime factors of m . Also, in what follows, we always only consider positive divisors of m . We define

$$S_m := \sum_{k=1}^m \langle \{0, \frac{k}{m}\}, f \rangle,$$

$$S'_m := \sum_{\substack{k=1 \\ (k, m)=1}}^m \langle \{0, \frac{k}{m}\}, f \rangle.$$

We repeatedly use the following identity.

Lemma 2.2. *For each odd square free positive integer $m > 1$, we have*

$$\sum_{l|m} S_l = \sum_{d=1}^{r(m)} 2^{r(m)-d} \sum_{\substack{n|m \\ r(n)=d}} S'_n.$$

Proof. We obviously have

$$\sum_{l|m} S_l = \sum_{l|m} \sum_{n|l} S'_n.$$

Now fix an integer d with $1 \leq d \leq r(m)$, and divisor n of m with $r(n) = d$. Then the number of divisors l of m , which are divisible by n , is equal to

$$\sum_{j=1}^{r(m)-d} \binom{r(m)-d}{j},$$

whence the assertion of the lemma follows. \square

If q is any prime of good reduction for E , we let a_q denote the trace of Frobenius at q , and define $N_q = q + 1 - a_q$. Thus N_q is the number of points on the reduction of E modulo q with coordinates in the field with q elements. Now suppose that $m = q_1 q_2 \cdots q_{r(m)}$ is an odd square free integer $m > 1$ with $(m, C) = 1$. The following identity is due to (2.1)

$$(2.3) \quad ((1 + q_1)(1 + q_2) \cdots (1 + q_{r(m)}) - a_{q_1} a_{q_2} \cdots a_{q_{r(m)}}) L(E, 1) = - \sum_{l|m} S_l.$$

As before, we write Ω^+ for the least positive real period of a Neron differential on global minimal equation for E .

Lemma 2.3. *Let E be a $\Gamma_0(C)$ -optimal elliptic curve over \mathbb{Q} , with $L(E, 1) \neq 0$ and $E[2](\mathbb{Q}) = 0$. Let m be an odd square free integer greater than 1 with $(m, C) = 1$. Assume that N_q is odd for each prime factor q of m . Then*

$$\text{ord}_2(S'_m/\Omega^+) = \text{ord}_2(L^{(alg)}(E, 1)).$$

Proof. We use induction on $r(m)$, the number of prime factors of m . Suppose first that $r(m) = 1$, say $m = q_1$. Then by (2.3), we have

$$N_{q_1} L(E, 1) = S'_{q_1},$$

and the assertion is then clear because N_{q_1} is odd. Now suppose $r(m) > 1$ and assume the lemma is true for all divisors $n > 1$ of m with $n \neq m$. Note also that $a_{q_1}, \dots, a_{q_{r(m)}}$ are all odd, and so

$$(1 + q_1)(1 + q_2) \cdots (1 + q_{r(m)}) - a_{q_1} a_{q_2} \cdots a_{q_{r(m)}}$$

is odd. Hence it follows from (2.3) that

$$\text{ord}_2(L^{(alg)}(E, 1)) = \text{ord}_2 \left(\sum_{l|m} S_l / \Omega^+ \right).$$

But, by Lemma 2.2, we have

$$\sum_{l|m} S_l / \Omega^+ = S'_m / \Omega^+ + \sum_{d=1}^{r(m)-1} 2^{r(m)-d} \sum_{\substack{n|m \\ r(n)=d}} S'_n / \Omega^+.$$

By our induction hypothesis, every term in the second sum on the right hand side of this equation has order strictly greater than $\text{ord}_2(L^{(alg)}(E, 1))$. Hence $\text{ord}_2(S'_m / \Omega^+) = \text{ord}_2(L^{(alg)}(E, 1))$, and the proof is complete. \square

Lemma 2.4. *Let E be a $\Gamma_0(C)$ -optimal elliptic curve over \mathbb{Q} with $\text{ord}_2(L^{(alg)}(E, 1)) = -1$. Let m be an odd square free integer greater than 1 with $(m, C) = 1$. Assume that $q \equiv 3 \pmod{4}$ and $N_q \equiv 2 \pmod{4}$ for each prime q dividing m . Then*

$$\text{ord}_2(S'_m / \Omega^+) = r(m) - 1.$$

Proof. When $r(m) = 1$, say $m = q_1$, the assertion of the lemma follows immediately from (2.3). Now assume $r(m) > 1$, and assume the lemma is true for all divisors $n > 1$ of m with $n \neq m$. Note also that $q \equiv 3 \pmod{4}$ and $N_q \equiv 2 \pmod{4}$ for each prime q dividing m , and so

$$\text{ord}_2((1 + q_1)(1 + q_2) \cdots (1 + q_{r(m)}) - a_{q_1} a_{q_2} \cdots a_{q_{r(m)}}) = r(m).$$

But, by Lemma 2.2, we have

$$(2.4) \quad \sum_{l|m} S_l/\Omega^+ = S'_m/\Omega^+ + \left(2 \sum_{\substack{n|m \\ r(n)=r(m)-1}} S'_n + 2^2 \sum_{\substack{n|m \\ r(n)=r(m)-2}} S'_n + \cdots + 2^{r(m)-1} \sum_{\substack{n|m \\ r(n)=1}} S'_n \right) / \Omega^+.$$

Suppose first that $r(m)$ is odd, by our induction hypothesis, it is easy to see that

$$\begin{aligned} & 2 \sum_{\substack{n|m \\ r(n)=r(m)-1}} S'_n/\Omega^+ + 2^{r(m)-1} \sum_{\substack{n|m \\ r(n)=1}} S'_n/\Omega^+, \\ & \quad \dots, \\ & 2^{\frac{r(m)-1}{2}} \sum_{\substack{n|m \\ r(n)=(r(m)+1)/2}} S'_n/\Omega^+ + 2^{\frac{r(m)+1}{2}} \sum_{\substack{n|m \\ r(n)=(r(m)-1)/2}} S'_n/\Omega^+ \end{aligned}$$

are all divisible by $2^{r(m)}$, so the sum of all the terms in the second part on the right hand side of (2.4) has order strictly greater than $r(m) - 1$. Also note that $\text{ord}_2(L^{(alg)}(E, 1)) = -1$, whence, it follows that $\text{ord}_2(S'_m/\Omega^+) = r(m) - 1$. We then suppose that $r(m)$ is even. By our induction hypothesis, it is easy to see that all

$$\begin{aligned} & 2 \sum_{\substack{n|m \\ r(n)=r(m)-1}} S'_n/\Omega^+ + 2^{r(m)-1} \sum_{\substack{n|m \\ r(n)=1}} S'_n/\Omega^+, \\ & 2^2 \sum_{\substack{n|m \\ r(n)=r(m)-2}} S'_n/\Omega^+ + 2^{r(m)-2} \sum_{\substack{n|m \\ r(n)=2}} S'_n/\Omega^+, \\ & \quad \dots, \\ & 2^{\frac{r(m)-2}{2}} \sum_{\substack{n|m \\ r(n)=(r(m)+2)/2}} S'_n/\Omega^+ + 2^{\frac{r(m)+2}{2}} \sum_{\substack{n|m \\ r(n)=(r(m)-2)/2}} S'_n/\Omega^+, \\ & \quad 2^{\frac{r(m)}{2}} \sum_{\substack{n|m \\ r(n)=r(m)/2}} S'_n/\Omega^+ \end{aligned}$$

are divisible by $2^{r(m)}$. Similarly, it follows that $\text{ord}_2(S'_m/\Omega^+) = r(m) - 1$. The proof of the lemma is complete. \square

Lemma 2.5. *Let E be a $\Gamma_0(C)$ -optimal elliptic curve over \mathbb{Q} , with $L(E, 1) \neq 0$. Let m be an odd square free integer greater than 1 with $(m, C) = 1$. Assume that $\text{ord}_2(N_q) + \text{ord}_2(L^{(alg)}(E, 1)) > 0$ for at least one prime factor q of m . Then*

$$\text{ord}_2(S'_m/\Omega^+) \geq 1.$$

Proof. The proof is similar to the above two proofs. We first note that

$$\text{ord}_2(S'_q/\Omega^+) = \text{ord}_2(N_q L^{(alg)}(E, 1)) \geq 1.$$

The lemma then follows easily by an induction on r . \square

In order to understand the 2-part of the Birch and Swinnerton-Dyer conjecture for $E^{(M)}$, we have to understand how the 2-part of the Tamagawa factors of $E^{(M)}$ vary for primes. We assume once again that $M \equiv 1 \pmod{4}$ is an arbitrary square free integer with $(M, C) = 1$. Note that $E^{(M)}$ has bad additive reduction at all primes dividing M . Write $c_q(E^{(M)})$ for the Tamagawa factor of $E^{(M)}$ at a finite odd prime q . We then have the following lemma, and one can find a detailed discussion in [4, §7].

Lemma 2.6. *For any odd prime $q \mid M$, we have that*

$$\text{ord}_2(c_q(E^{(M)})) = \text{ord}_2(\#E(\mathbb{Q}_q)[2]).$$

Proposition 2.7. *Let E be an elliptic curve over \mathbb{Q} , with $E[2](\mathbb{Q}) = 0$. Let M be any integer of the form $M = \pm q_1 q_2 \cdots q_r$, where $r \geq 1$, q_1, \dots, q_r are arbitrary distinct odd primes which are inert in the field F . Then we have*

$$\text{ord}_2(c_{q_i}(E^{(M)})) = 0$$

for any integer $1 \leq i \leq r$.

Proof. Note that $E[2](\mathbb{Q}) = 0$ and q_i ($1 \leq i \leq r$) is inert in F , so $\#E(\mathbb{Q}_{q_i})[2]$ must be an odd integer. It then follows easily by the above lemma. \square

3. PERIOD LATTICE AND THE PROOF OF NON-VANISHING RESULTS

In this section, we prove the non-vanishing results of Section 1 combining the crucial lemmas in the previous section with some elementary facts on the period lattice of elliptic curves.

When the discriminant of E is negative, then $E(\mathbb{R})$ has only one real component, and so the period lattice \mathfrak{L} of the Néron differential on E has a \mathbb{Z} -basis of the form

$$\left[\Omega^+, \frac{\Omega^+ + i\Omega^-}{2} \right].$$

When the discriminant of E is positive, then $E(\mathbb{R})$ has two real components, and so the period lattice \mathfrak{L} of the Néron differential on E has a \mathbb{Z} -basis of the form

$$[\Omega^+, i\Omega^-].$$

One can find detailed descriptions of the period lattice of elliptic curves in Cremona's book [5, Chapter 2].

Now we give the proof of our theorems. We use the same notations as before, and denote $m = M/\epsilon > 0$ in what follows of this section.

Proof of Theorem 1.1. Firstly, as $E[2](\mathbb{Q}) = 0$ and q_1, q_2, \dots, q_r are totally inert in F , then we have that $\#E(\mathbb{F}_{q_i})[2] = 0$, that means the order of $E(\mathbb{F}_{q_i})$ must be odd, where $1 \leq i \leq r$. So a_i is odd by applying $a_q = q+1 - \#A(\mathbb{F}_q)$, i.e. N_{q_i} is odd for any $1 \leq i \leq r$. Secondly, as E has negative discriminant, we can write

$$\langle \{0, \frac{k}{m}\}, f \rangle = (s_k \Omega^+ + it_k \Omega^-)/2$$

for any integer m coprime to C , where s_k, t_k are integers of the same parity. Moreover, by the basic property of modular symbols, $\langle \{0, \frac{k}{m}\}, f \rangle$ and $\langle \{0, \frac{m-k}{m}\}, f \rangle$ are complex conjugate periods of E . Thus we obtain

$$S'_m/\Omega^+ = \sum_{\substack{k=1 \\ (k,m)=1}}^{(m-1)/2} s_k.$$

Then by Lemma 2.3, it follows that

$$\sum_{\substack{k=1 \\ (k,m)=1}}^{(m-1)/2} s_k$$

is an odd integer. On the other hand, according to (2.2), we have that

$$\sqrt{M}L(A^{(M)}, 1) = \sum_{k=1}^m \chi(k) \langle \{0, \frac{k}{m}\}, f \rangle.$$

When $M > 0$, i.e. $\epsilon = 1$, noting that $\chi(k) = \chi(m-k)$, it follows easily that

$$\sqrt{M}L(A^{(M)}, 1)/\Omega^+ = \sum_{k=1}^{(m-1)/2} \chi(k) s_k \equiv \sum_{\substack{k=1 \\ (k,m)=1}}^{(m-1)/2} s_k \pmod{2}.$$

The last congruence holds because $\chi(k) \equiv 1 \pmod{2}$ when $(k, m) = 1$, and $\chi(k) = 0$ when $(k, m) > 1$. The assertion of the theorem now follows when $M > 0$.

When $M < 0$, i.e. $\epsilon = -1$, noting that $\chi(k) = -\chi(m-k)$, it follows easily that

$$\sqrt{M}L(A^{(M)}, 1)/(i\Omega^-) = \sum_{k=1}^{(m-1)/2} \chi(k)t_k \equiv \sum_{\substack{k=1 \\ (k,m)=1}}^{(m-1)/2} t_k \equiv \sum_{\substack{k=1 \\ (k,m)=1}}^{(m-1)/2} s_k \pmod{2}.$$

The last congruence holds because $\chi(k) \equiv 1 \pmod{2}$ when $(k, m) = 1$, and $\chi(k) = 0$ when $(k, m) > 1$, and noting that s_k, t_k are of the same parity. The assertion of the theorem now follows when $M < 0$.

Hence

$$\text{ord}_2(L^{(alg)}(E^{(M)}, 1)) = 0$$

for both cases. This completes the proof of Theorem 1.1.

The proof of Theorem 1.2 is similar to the proof of 1.1.

Proof of Theorem 1.2. Since E has positive discriminant, we can write

$$\langle \{0, \frac{k}{m}\}, f \rangle = s_k \Omega^+ + it_k \Omega^-$$

for any integer m coprime to C , where s_k, t_k are integers, but are independent with the ones in the above proof. Then by Lemma 2.3, it follows that

$$\text{ord}_2 \left(2 \sum_{\substack{k=1 \\ (k,m)=1}}^{(m-1)/2} s_k \right) = \text{ord}_2(L^{(alg)}(E, 1)) = 1.$$

Thus

$$\sum_{\substack{k=1 \\ (k,m)=1}}^{(m-1)/2} s_k$$

is an odd integer. Noting that $\chi(k) = \chi(m-k)$, it follows easily that

$$\sqrt{M}L(A^{(M)}, 1)/\Omega^+ = 2 \sum_{k=1}^{(m-1)/2} \chi(k)s_k \equiv 2 \sum_{\substack{k=1 \\ (k,m)=1}}^{(m-1)/2} s_k \pmod{4}.$$

Hence

$$\text{ord}_2(L^{(alg)}(E^{(M)}, 1)) = 1.$$

This completes the proof of Theorem 1.2.

We remark here that when the discriminant of E is negative and $E[2](\mathbb{Q}) = 0$, we must have $\text{ord}_2(L^{(alg)}(E, 1)) \geq 0$; and when the discriminant of E is positive and $E[2](\mathbb{Q}) = 0$, we must have $\text{ord}_2(L^{(alg)}(E, 1)) \geq 1$. These assertions could be easily seen from the proofs of Theorem 1.1 and Theorem 1.2.

We now prove Theorem 1.3 and Theorem 1.5.

When E has negative discriminant and $\text{ord}_2(L^{(alg)}(E, 1)) + \text{ord}_2(N_q) = 0$, we have that

$$\text{ord}_2 \left(\sum_{k=1}^{(q-1)/2} s_k \right) = \text{ord}_2(N_q L^{(alg)}(E, 1)) = 0.$$

Theorem 1.3 then follows by the same argument in the proof of Theorem 1.1.

When E has negative discriminant and $\text{ord}_2(L^{(alg)}(E, 1)) + \text{ord}_2(N_q) = 1$, we have that

$$\text{ord}_2 \left(2 \sum_{k=1}^{(q-1)/2} s_k \right) = \text{ord}_2(N_q L^{(alg)}(E, 1)) = 1.$$

Thus

$$\sum_{k=1}^{(q-1)/2} s_k$$

is an odd integer. Theorem 1.5 then follows by the same argument in the proof of Theorem 1.2.

We now prove Theorem 1.6 and Theorem 1.7.

When E has negative discriminant and $\text{ord}_2(L^{(\text{alg})}(E, 1)) + \text{ord}_2(N_{q_i}) > 0$, we have that

$$\text{ord}_2 \left(\sum_{\substack{k=1 \\ (k,m)=1}}^{(m-1)/2} s_k \right) \geq 1$$

by Lemma 2.5. Thus

$$\sum_{\substack{k=1 \\ (k,m)=1}}^{(m-1)/2} s_k$$

is even. Then both

$$\sum_{k=1}^{(m-1)/2} \chi(k)s_k \quad \text{and} \quad \sum_{k=1}^{(m-1)/2} \chi(k)t_k$$

are even. So we have

$$\text{ord}_2(L^{(\text{alg})}(E^{(M)}, 1)) = \text{ord}_2 \left(\sum_{k=1}^{(m-1)/2} \chi(k)s_k \right) \geq 1$$

when $M > 0$, and

$$\text{ord}_2(L^{(\text{alg})}(E^{(M)}, 1)) = \text{ord}_2 \left(\sum_{k=1}^{(m-1)/2} \chi(k)t_k \right) \geq 1$$

when $M < 0$. This proves Theorem 1.6.

When E has positive discriminant, of course we have

$$\text{ord}_2(L^{(\text{alg})}(E^{(M)}, 1)) = \text{ord}_2 \left(2 \sum_{k=1}^{(m-1)/2} \chi(k)s_k \right) \geq 1$$

when $M > 0$, and

$$\text{ord}_2(L^{(\text{alg})}(E^{(M)}, 1)) = \text{ord}_2 \left(2 \sum_{k=1}^{(m-1)/2} \chi(k)t_k \right) \geq 1$$

when $M < 0$. This proves Theorem 1.7.

4. QUADRATIC TWISTS OF NEUMANN-SETZER ELLIPTIC CURVES

In this section, we shall take the Neumann-Setzer elliptic curves as an example of Theorem 1.3, and verify the 2-part of Birth and Swinnerton-Dyer conjecture for a family of quadratic twist of the curves.

Let p be a prime of the form $u^2 + 64$ for some integer u , which is congruent to 1 modulo 4. According to Neumann [11][12] and Setzer [14], there are just two elliptic curves of conductor p , up to isomorphism, namely,

$$\begin{aligned} A : \quad y^2 + xy &= x^3 + \frac{u-1}{4}x^2 + 4x + u, \\ A' : \quad y^2 + xy &= x^3 - \frac{u-1}{4}x^2 - x. \end{aligned}$$

The curves A and A' are 2-isogenous and of which the Mordell-Weil groups are both $\mathbb{Z}/2\mathbb{Z}$. The discriminant of A is $-p^2$, and the discriminant of A' is p . We denote F and F' to be the 2-division fields of A and A' , respectively. It is easy to get that

$$\mathbb{Q}(A[2]) = \mathbb{Q}(i), \quad \mathbb{Q}(A'[2]) = \mathbb{Q}(\sqrt{p}).$$

Let $X_0(p)$ be the modular curve of level p , and there is a non-constant rational map $X_0(p) \rightarrow A$, of which the modular parametrization is $\Gamma_0(p)$ -optimal by Mestre and Oesterlé [10].

4.1. Classical 2-descents. In order to carry out the 2-descent, we must work with a new equation for A and its twists. Making change of variables, we obtain the following equation for A :

$$Y^2 = X^3 - 2uX^2 + pX.$$

Let M be any square free integer $\neq 1$, and let $A^{(M)}$ be the twist of M by the quadratic extension $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$. Then the curve $A^{(M)}$ will have equation

$$A^{(M)} : y^2 = x^3 - 2uMx^2 + pM^2x.$$

and, dividing this curve by the subgroup generated by the point $(0, 0)$, we obtain the new curve

$$A'^{(M)} : y^2 = x^3 + 4uMx^2 - 256M^2x.$$

Explicitly, the isogenies between these two curves, are given by

$$\begin{aligned} \phi : A^{(M)} &\rightarrow A'^{(M)}, (x, y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(pM^2 - x^2)}{x^2} \right); \\ \hat{\phi} : A'^{(M)} &\rightarrow A^{(M)}, (x, y) \mapsto \left(\frac{y^2}{4x^2}, \frac{y(-256M^2 - x^2)}{8x^2} \right). \end{aligned}$$

We write $S^{(\phi)}(A^{(M)})$ and $S^{(\hat{\phi})}(A'^{(M)})$ for the classical Selmer groups of the isogenies ϕ and $\hat{\phi}$, which can be described explicitly as follows. Let V denote the set of all places of \mathbb{Q} , and let T_M be the set of primes dividing $2pM$. Let $\mathbb{Q}(2, M)$ be the subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ consisting of all elements with a representative which has even order at each prime number not in T_M . Writing

$$(4.1) \quad C_d : dw^2 = 4p - \left(\frac{M}{d}z^2 - 2u \right)^2,$$

then $S^{(\phi)}(A^{(M)})$ can be naturally identified with the subgroup of all d in $\mathbb{Q}(2, M)$ such that $C_d(\mathbb{Q}_v)$ is non-empty for $v = \infty$ and v dividing $2pM$. Similarly, writing

$$(4.2) \quad C'_d : dw^2 = 64p^3 + p \left(\frac{M}{d}z^2 - up \right)^2,$$

then $S^{(\hat{\phi})}(A'^{(M)})$ can be naturally identified with the subgroup of all d in $\mathbb{Q}(2, M)$ such that $C'_d(\mathbb{Q}_v)$ is non-empty for $v = \infty$ and v dividing $2pM$. Note that $-1 \in S^{(\phi)}(A^{(M)})$ because it is the image of the point $(0, 0)$ in $A'^{(M)}(\mathbb{Q})$, and similarly $p \in S^{(\hat{\phi})}(A'^{(M)})$ (see Proposition 4.9 of [15]).

If D is any odd square free integer, we define D_+ (resp. D_-) to be the product of the primes dividing D , which are $\equiv 1 \pmod{4}$ (resp. which are $\equiv 3 \pmod{4}$). In what follows, we shall always assume that M is an odd square free integer which is prime to p , and let R denote the product of the prime factors of M which are inert in the field $\mathbb{Q}(\sqrt{p})$, and let N denote the product of prime factors of M which split in the field $\mathbb{Q}(\sqrt{p})$, and let $\left(\frac{\cdot}{q} \right)$ be the Jacobi symbol. We will then write $M = \epsilon RN$, where $\epsilon = \pm 1$.

Proposition 4.1. *Let M be an odd square free integer which is prime to p . Then $S^{(\phi)}(A^{(M)})$ consists of the classes in $\mathbb{Q}(2, M)$ represented by all integers $d, -d$ satisfying the following conditions:*

- (1) d divides N ;
- (2) $\left(\frac{d}{q} \right) = 1$ for all primes q dividing $M_+/(M_+, d)$, and $\left(\frac{M/d}{q} \right) = \left(\frac{2u+2a}{q} \right)$ for all primes q dividing (N_+, d) , where a is an integer satisfying $a^2 \equiv p \pmod{q}$.

Proof. We recall that C_d denotes the curve (4.1). We see immediately that $C_d(\mathbb{R}) \neq \emptyset$.

If 2 divides d , a point on C_d with coordinates in \mathbb{Q}_2 must have coordinates in \mathbb{Z}_2 , whence it follows easily that $C_d(\mathbb{Q}_2) = \emptyset$. If p divides d , a point on C_d with coordinates in \mathbb{Q}_p must have coordinates in \mathbb{Z}_p , whence it follows easily that $C_d(\mathbb{Q}_p) = \emptyset$. So next we need only to consider the cases when $2 \nmid d$ and $p \nmid d$.

We claim that

$$(4.3) \quad C_d(\mathbb{Q}_2) \neq \emptyset$$

is always true for any odd integer d . Note that (4.1) has a solution in \mathbb{Q}_2 with $w = 0$ for any M/d . So our claim follows.

We now determine when

$$(4.4) \quad C_d(\mathbb{Q}_p) \neq \emptyset.$$

We shall prove that (4.4) is true if and only if $\left(\frac{d}{p}\right) = 1$. Note first that (4.1) has a solution in \mathbb{Q}_p with $z = 0$ if and only if $\left(\frac{d}{p}\right) = 1$, and there is no solution when $w = 0$. We then put $w = p^{-m}w_1, z = p^{-n}z_1$, where $m, n > 0$, and w_1, z_1 are in \mathbb{Z}_p^\times . Then a necessary condition for a solution is that $m = 2n$, and we then obtain the new equation

$$dw_1^2 = 4p^{4n+1} - \left(\frac{M}{d}z_1^2 - 2up^{2n}\right)^2,$$

which is soluble modulo p if and only if $\left(\frac{-d}{p}\right) = 1$, i.e. $\left(\frac{d}{p}\right) = 1$. Next we put $w = p^m w_1, z = p^n z_1$, where $m, n \geq 0$, and w_1, z_1 are in \mathbb{Z}_p^\times , the equation then becomes

$$dw_1^2 = \frac{4p - (p^{2n}\frac{M}{d}z_1^2 - 2u)^2}{p^{2m}}.$$

It follows easily that we must have $m = 0$ and $n \geq 0$. For $m = 0$ and $n = 0$, the equation becomes

$$dw_1^2 = 4p - \left(p^{2n}\frac{M}{d}z_1^2 - 2u\right)^2.$$

Taking the above equation modulo p , and then we have that it is soluble in \mathbb{Q}_p if and only if $\left(\frac{d}{p}\right) = 1$. This proves our claim for (4.4).

We now determine when

$$(4.5) \quad C_d(\mathbb{Q}_q) \neq \emptyset,$$

where q is a prime factor of M . Assume first that q divides d . We claim that (4.5) is always true when $q \mid N_-$ and is true if and only if $\left(\frac{M/d}{q}\right) = \left(\frac{2u+2a}{q}\right)$ when $q \mid N_+$, where a is an integer satisfying $a^2 \equiv p \pmod{q}$. Indeed, a point on C_d with coordinates in \mathbb{Q}_q must have coordinates in \mathbb{Z}_q . Taking the equation of C_d modulo q , it then becomes

$$4p - \left(\frac{M}{d}z^2 - 2u\right)^2 \equiv 0 \pmod{q}.$$

It is easy to see that a necessary condition for the solubility is $\left(\frac{p}{q}\right) = 1$. We assume this and $a^2 \equiv p \pmod{q}$, then the equation becomes

$$\frac{M}{d}z^2 \equiv 2u \pm 2a \pmod{q}.$$

Note that $(2u + 2a)(2u - 2a) \equiv -256 \pmod{q}$ and $\left(\frac{-1}{q}\right) = -1$ when $q \equiv 3 \pmod{4}$, so (4.5) will always be true when q divides N_- , and it will be true when q divides N_+ if and only if $\left(\frac{M/d}{q}\right) = \left(\frac{2u+2a}{q}\right)$. This proves our claim. Now assume that q does not divide d . We claim that (4.5) is always true when $q \mid M_-$ and is true if and only if $\left(\frac{d}{q}\right) = 1$ when $q \mid M_+$. Indeed, if $\left(\frac{d}{q}\right) = 1$, the congruence given by putting $z = 0$ in the equation of C_d modulo q is clearly soluble, and this gives a point on C_d with coordinates in \mathbb{Z}_q . Conversely, if there is a point on C_d with coordinates in \mathbb{Z}_q , it follows immediately that $\left(\frac{d}{q}\right) = 1$. On the other hand, if there is a point (w, z) on C_d with non-integral coordinates, we can write $w = q^{-m}w_1, z = q^{-n}z_1$ with $m, n > 0$ and $w_1, z_1 \in \mathbb{Z}_q^\times$. It then follows that $m = 2n - 1$ and the equation becomes

$$dw_1^2 = 4pq^{2m} - \left(\frac{M}{qd}z_1^2 - 2uq^m\right)^2.$$

Taking this last equation modulo q , we conclude that $\left(\frac{d}{q}\right) = \left(\frac{-1}{q}\right)$. Our claim then follows.

Putting together all of the above results, the proof of Proposition 4.1 is complete. \square

Proposition 4.2. *Let M be an odd square free integer which is prime to p . Then $S^{(\hat{\phi})}(A'^{(M)})$ consists of the classes in $\mathbb{Q}(2, M)$ represented by all integers d, pd satisfying the following conditions:*

- (1) d divides M_+ and $d > 0$;
- (2) $d \equiv 1 \pmod{4}$ when $M \equiv 1 \pmod{4}$, and $d \equiv 1 \pmod{8}$ when $M \equiv 3 \pmod{4}$;

- (3) $\left(\frac{d}{q}\right) = 1$ for all primes q dividing $N/(N, d)$, and $\left(\frac{M/d}{q}\right) = \left(\frac{u+8b}{q}\right)$ for all primes q dividing (N_+, d) , where b is an integer satisfying $b^2 \equiv -1 \pmod{q}$.

Proof. We recall that C'_d denotes the curve (4.2). It is clear that $C'_d(\mathbb{R}) \neq \emptyset$ if and only if $d > 0$.

If 2 divides d , a point on C'_d with coordinates in \mathbb{Q}_2 must have coordinates in \mathbb{Z}_2 , whence it follows easily that $C'_d(\mathbb{Q}_2) = \emptyset$. So next we need only to consider the case when $2 \nmid d$.

We claim that

$$(4.6) \quad C'_d(\mathbb{Q}_2) \neq \emptyset$$

is true if and only if $d \equiv 1 \pmod{4}$ when $M \equiv 1 \pmod{4}$, and $d \equiv 1 \pmod{8}$ when $M \equiv 3 \pmod{4}$. Note first that (4.2) has a solution in \mathbb{Q}_2 with $z = 0$ if and only if $d \equiv 1 \pmod{8}$, (4.2) has no solution in \mathbb{Q}_2 with $w = 0$. Put $w = 2^{-m}w_1, z = 2^{-n}z_1$, where $m, n > 0$, and w_1, z_1 are in \mathbb{Z}_2^\times . Then a necessary condition for a solution is that $m = 2n$, and we then obtain the new equation

$$dw_1^2 = 2^{4n+6}p^3 + p \left(\frac{M}{d}z_1^2 - 2^{2n}up \right)^2.$$

Taking the above equation modulo 8, it follows that it has a solution in \mathbb{Q}_2 if and only if $d \equiv 1 \pmod{8}$. Next we put $w = 2^m w_1, z = 2^n z_1$, where $m, n \geq 0$, and w_1, z_1 are in \mathbb{Z}_2^\times , the equation then becomes

$$dw_1^2 = \frac{64p^3 + p \left(2^{2n} \frac{M}{d} z_1^2 - up \right)^2}{2^{2m}}.$$

It follows easily that we have either $m = 0$ and $n \geq 1$, or $m \geq 1$ and $n = 0$. For $m = 0$ and $n \geq 1$, the equation becomes

$$dw_1^2 = 64p^3 + p \left(2^{2n} \frac{M}{d} z_1^2 - up \right)^2.$$

By taking the above equation modulo 8, we have that it is soluble in \mathbb{Q}_2 if and only if $d \equiv 1 \pmod{8}$. For $m \geq 1$ and $n = 0$, the equation becomes

$$dw_1^2 = \frac{64p^3 + p \left(\frac{M}{d} z_1^2 - up \right)^2}{2^{2m}}.$$

When $m = 1$, necessarily we have that $\frac{M}{d} z_1^2 - up \equiv 2 \pmod{4}$, i.e. $M/d \equiv 3 \pmod{4}$, implying $d \equiv 1 \pmod{8}$. When $m = 2$, necessarily we have that $\frac{M}{d} z_1^2 - up \equiv 4 \pmod{8}$, i.e. $M/d \equiv 5 \pmod{8}$ when $p \equiv 1 \pmod{16}$ and $M/d \equiv 1 \pmod{8}$ when $p \equiv 9 \pmod{16}$, implying $d \equiv 5 \pmod{8}$. When $m = 3$, necessarily we have that $\text{ord}_2 \left(\frac{M}{d} z_1^2 - up \right) \geq 4$, i.e. $M/d \equiv 1 \pmod{8}$ when $p \equiv 1 \pmod{16}$ and $M/d \equiv 5 \pmod{8}$ when $p \equiv 9 \pmod{16}$, implying $d \equiv 1 \pmod{4}$. When $m \geq 4$, necessarily we have that $\frac{M}{d} z_1^2 - up \equiv 8 \pmod{16}$ and $\text{ord}_2 \left(p^3 + p \left(\frac{\frac{M}{d} z_1^2 - up}{8} \right)^2 \right) = 2m - 6$, but $\text{ord}_2 \left(p^3 + p \left(\frac{\frac{M}{d} z_1^2 - up}{8} \right)^2 \right) = 1$ as $\left(\frac{\frac{M}{d} z_1^2 - up}{8} \right)^2 \equiv 1 \pmod{8}$, which is a contradiction. Combining those cases above, we can see that (4.2) is soluble in \mathbb{Q}_2 if and only if $d \equiv 1 \pmod{4}$ when $M \equiv 1 \pmod{4}$, and $d \equiv 1 \pmod{8}$ when $M \equiv 3 \pmod{4}$. This proves our claim for (4.6).

We now determine when

$$(4.7) \quad C'_d(\mathbb{Q}_p) \neq \emptyset.$$

We shall prove that (4.7) is always true. When p divides d , we put $d = pd_1$, then (4.2) becomes

$$d_1 w^2 = 64p^2 + \left(\frac{M}{pd_1} z^2 - up \right)^2.$$

Note first that (4.2) has no solution in \mathbb{Q}_p with $wz = 0$. We put $w = p^{-m}w_1, z = p^{-n+1}z_1$, where $m, n > 0$, and w_1, z_1 are in \mathbb{Z}_p^\times . Then a necessary condition for a solution is that $m = 2n - 1$, and we then obtain the new equation

$$d_1 w_1^2 = 64p^{2m+2} + \left(\frac{M}{d_1} z_1^2 - up^{m+1} \right)^2.$$

Taking the above equation modulo p , it follows that it has a solution in \mathbb{Q}_p if and only if $\left(\frac{d_1}{p}\right) = 1$. Next we put $w = p^m w_1, z = p^{n+1} z_1$, where $m, n \geq 0$, and w_1, z_1 are in \mathbb{Z}_p^\times , the equation then becomes

$$d_1 w_1^2 = \frac{64 + \left(p^{2n} \frac{M}{d_1} z_1^2 - u\right)^2}{p^{2m-2}}.$$

It follows that we must have $m \geq 1, n = 0$. Taking $m = 1$ and $n = 0$, the equation becomes

$$d_1 w_1^2 = 64 + \left(\frac{M}{d_1} z_1^2 - u\right)^2.$$

Taking the above equation modulo p , we have $d_1 w_1^2 \equiv \frac{M}{d_1} z_1^2 \left(\frac{M}{d_1} z_1^2 - 2u\right) \pmod{p}$, which is always soluble with proper z and w . That means (4.7) is always true when $p \mid d$. Now we assume that p does not divide d . we see that (4.7) will be true if and only if C'_d has a point with coordinates in \mathbb{Z}_p . Next we put $w = p^m w_1, z = p^n z_1$, where $m, n \geq 0$, and w_1, z_1 are in \mathbb{Z}_p^\times , the equation then becomes

$$dw_1^2 = \frac{p^{4n+1} \frac{M^2}{d^2} z_1^4 - 2up^{2n+2} \frac{M}{d} z_1^2 + p^4}{p^{2m}}.$$

It follows that we have either $m = 2$ and $n \geq 1$, or $m \geq 3$ and $n = 1$. Taking $m = 2$ and $n = 1$, and taking the above equation modulo p , we have that $dw_1^2 \equiv 1 - 2u \frac{M}{d} z_1^2 \pmod{p}$, which is always soluble with proper z and w . That means (4.7) is always true when $p \nmid d$. Our claim for (4.7) then follows.

Finally, we must determine when

$$(4.8) \quad C'_d(\mathbb{Q}_q) \neq \emptyset,$$

where q is a prime factor of M . Assume first that q divides d . We claim that (4.8) is true if and only if $\left(\frac{M/d}{q}\right) = \left(\frac{u+8b}{q}\right)$, where b is an integer satisfying $b^2 \equiv -1 \pmod{q}$. Indeed, a point on C'_d with coordinates in \mathbb{Q}_q must have coordinates in \mathbb{Z}_q . Taking the equation of C'_d modulo q , it then becomes

$$\left(\frac{M}{d} z^2 - up\right)^2 \equiv -64p^2 \pmod{q}.$$

A necessary condition for a solution is that $q \equiv 1 \pmod{4}$. We now assume this condition and $b^2 \equiv -1 \pmod{q}$, then the above equation becomes

$$\frac{M}{d} z^2 \equiv up \pm 8pb \pmod{q},$$

Note that $(up + 8pb)(up - 8pb) \equiv p^3 \pmod{q}$, so (4.8) will always be true when $\left(\frac{p}{q}\right) = -1$, i.e. q divides R_+ , and it will be true when q divides N_+ if and only if $\left(\frac{M/d}{q}\right) = \left(\frac{u+8b}{q}\right)$. This proves our claim. Now assume that q does not divide d . We claim that (4.8) is always true when $q \mid R$ and is true if and only if $\left(\frac{d}{q}\right) = 1$ when $q \mid N$. Indeed, if $\left(\frac{d}{q}\right) = 1$, the congruence given by putting $z = 0$ in the equation of C'_d modulo q is clearly soluble, and this gives a point on C'_d with coordinates in \mathbb{Z}_q . Conversely, if there is a point on C'_d with coordinates in \mathbb{Z}_q , it follows immediately that $\left(\frac{d}{q}\right) = 1$. On the other hand, if there is a point (w, z) on C'_d with non-integral coordinates, we can write $w = q^{-m} w_1, z = q^{-n} z_1$ with $m, n > 0$ and $w_1, z_1 \in \mathbb{Z}_q^\times$. It then follows that $m = 2n - 1$ and the equation becomes

$$dw_1^2 = 64p^3 q^{2m} + p \left(\frac{M}{qd} z_1^2 - upq^m\right)^2.$$

Taking this last equation modulo q , we conclude that $\left(\frac{d}{q}\right) = \left(\frac{p}{q}\right)$. Our claim then follows.

Putting together all of the above results, the proof of Proposition 4.2 is complete. \square

We now give some consequences of Propositions 4.1 and 4.2. Assume for the rest of this paragraph that M is a square free integer, prime to p , with $M \equiv 1 \pmod{4}$. In particular, it follows that the curve $A^{(M)}$ always has good reduction at 2. When $M > 0$, its L -function has global root number $+1$ (reps. -1) if $\left(\frac{M}{p}\right) = 1$ (resp. $\left(\frac{M}{p}\right) = -1$), when $M < 0$, its L -function has global root number $+1$ (reps. -1)

if $\left(\frac{M}{p}\right) = -1$ (resp. $\left(\frac{M}{p}\right) = 1$). We write $S^{(2)}(A^{(M)})$ for the classical Selmer group of $A^{(M)}$ for the endomorphism given by multiplication by 2. Now it is easily seen that we have an exact sequence

$$0 \rightarrow \frac{A'^{(M)}(\mathbb{Q})[\hat{\phi}]}{\phi(A^{(M)}(\mathbb{Q})[2])} \rightarrow S^{(\phi)}(A^{(M)}) \rightarrow S^{(2)}(A^{(M)}) \rightarrow S^{(\hat{\phi})}(A'^{(M)}).$$

Define $\mathfrak{S}^{(\phi)}(A^{(M)})$, $\mathfrak{S}^{(\hat{\phi})}(A'^{(M)})$, $\mathfrak{S}^{(2)}(A^{(M)})$ and $\mathfrak{S}^{(2)}(A'^{(M)})$ to be the quotients of $S^{(\phi)}(A^{(M)})$, $S^{(\hat{\phi})}(A'^{(M)})$, $S^{(2)}(A^{(M)})$ and $S^{(2)}(A'^{(M)})$ by the images of the torsion subgroups of $A'^{(M)}(\mathbb{Q})$, $A^{(M)}(\mathbb{Q})$, $A^{(M)}(\mathbb{Q})$ and $A'^{(M)}(\mathbb{Q})$, respectively. By the fact that the 2-primary subgroups of $A'^{(M)}(\mathbb{Q})$ and $A^{(M)}(\mathbb{Q})$ are both just of order 2, whence it follows easily that we have the exact sequence

$$(4.9) \quad 0 \rightarrow \mathfrak{S}^{(\phi)}(A^{(M)}) \rightarrow \mathfrak{S}^{(2)}(A^{(M)}) \rightarrow S^{(\hat{\phi})}(A'^{(M)}),$$

$$(4.10) \quad 0 \rightarrow \mathfrak{S}^{(\hat{\phi})}(A'^{(M)}) \rightarrow \mathfrak{S}^{(2)}(A'^{(M)}) \rightarrow S^{(\phi)}(A^{(M)}).$$

Note also that the parity theorem of the Dokchitser brothers [7] shows that $\mathfrak{S}^{(2)}(A^{(M)})$ has even or odd \mathbb{F}_2 -dimension according as the root number is $+1$ or -1 .

We now let $r(M)$, $k(M)$, $r_+(M)$, $r_-(M)$, $k_+(M)$, $k_-(M)$ denote the number of prime factors of R , N , R_+ , R_- , N_+ , N_- , respectively, and prove the following results.

Corollary 4.3. *Assume that $M = \epsilon R_- \equiv 1 \pmod{4}$, where $\epsilon = \pm 1$. Then $\mathfrak{S}^{(2)}(A^{(M)}) = 0$.*

Proof. Indeed Proposition 4.1 shows that, in this case, we have $\mathfrak{S}^{(\phi)}(A^{(M)}) = 0$, and Proposition 4.2 shows that $S^{(\hat{\phi})}(A'^{(M)})$ has order 2, whence the assertion follows from the exact sequence (4.9), and the fact that $\mathfrak{S}^{(2)}(A^{(M)})$ must have even \mathbb{F}_2 -dimension. Note that, of course, $r_-(M)$ has to be even when $\epsilon = 1$, and $r_-(M)$ has to be odd when $\epsilon = -1$. \square

Corollary 4.4. *Assume that $M = N_- \equiv 1 \pmod{4}$. Then $\mathfrak{S}^{(\phi)}(A^{(M)})$ has exact order $2^{k_-(M)}$, and $\mathfrak{S}^{(2)}(A^{(M)})$ has exact order $2^{k_-(M)}$.*

Proof. The first assertion is clear from Proposition 4.1. Proposition 4.2 shows that $S^{(\hat{\phi})}(A'^{(M)})$ has order 2. So the corollary is clear from the exact sequence (4.9). Note that, of course, $k_-(M)$ has to be even since $M \equiv 1 \pmod{4}$. \square

Corollary 4.5. *Assume that $M = -p_0 R_- \equiv 1 \pmod{4}$, where p_0 is a prime congruent to 3 modulo 4 and splitting in $\mathbb{Q}(\sqrt{p})$. Then $\mathfrak{S}^{(\phi)}(A^{(M)})$ has exact order 2, and $\mathfrak{S}^{(2)}(A^{(M)})$ has exact order 2.*

Proof. The first assertion is clear from Proposition 4.1. Proposition 4.2 shows that $S^{(\hat{\phi})}(A'^{(M)})$ has order 2, whence the assertion follows from the exact sequence (4.9), and the fact that $\mathfrak{S}^{(2)}(A^{(M)})$ must have odd \mathbb{F}_2 -dimension. Note that, of course, $r_-(M)$ has to be even since $M \equiv 1 \pmod{4}$. \square

Corollary 4.6. *Assume that $M = q_0 R_- \equiv 1 \pmod{4}$, where q_0 is a prime congruent to 1 modulo 4 and inert in $\mathbb{Q}(\sqrt{p})$. Then $\mathfrak{S}^{(\phi)}(A^{(M)})$ has exact order 2, and $\mathfrak{S}^{(2)}(A'^{(M)})$ has exact order 2.*

Proof. The first assertion is clear from Proposition 4.2. Proposition 4.1 shows that $S^{(\phi)}(A^{(M)})$ has order 2, whence the assertion follows from the exact sequence (4.10), and the fact that $\mathfrak{S}^{(2)}(A'^{(M)})$ must have odd \mathbb{F}_2 -dimension. Note that, of course, $r_-(M)$ has to be even since $M \equiv 1 \pmod{4}$. \square

We now give the Tamagawa factors for the curves $A^{(M)}$ and $A'^{(M)}$, with a brief indication of proofs. We assume once again that M is an arbitrary square free integer, and write D_M for the discriminant of the field $\mathbb{Q}(\sqrt{M})$. Note that both $A^{(M)}$ and $A'^{(M)}$ have bad additive reduction at all primes dividing pD_M . Write $c_p(A^{(M)})$ for the Tamagawa factor of $A^{(M)}$ at a finite prime p , and similarly for $A'^{(M)}$. If q is an odd prime of bad additive reduction, we have

$$(4.11) \quad \text{ord}_2(c_q(A^{(M)})) = \text{ord}_2(\#A(\mathbb{Q}_q)[2]), \text{ord}_2(c_q(A'^{(M)})) = \text{ord}_2(\#A'(\mathbb{Q}_q)[2])$$

by Lemma 2.6. We then have the following propositions.

Proposition 4.7. *For all odd square free integers M , we have (i) $A^{(M)}(\mathbb{R})$ has one connected component, (ii) $c_p(A^{(M)}) = 2$, (iii) $c_q(A^{(M)}) = 2$ if $q \equiv 3 \pmod{4}$, and (iv) $c_q(A^{(M)}) = 4$ if $q \equiv 1 \pmod{4}$.*

Proof. Assertion (i) follows immediately from the fact that $\mathbb{Q}(A[2]) = \mathbb{Q}(i)$. The remaining assertions involving odd primes q of bad reduction follow immediately from (4.11), on noting that $A(\mathbb{Q}_q)[2]$ is of order 2 or 4, according as p does not or does split in $\mathbb{Q}(i)$, respectively. \square

Proposition 4.8. *For all odd square free integers M , we have (i) $A'^{(M)}(\mathbb{R})$ has two connected components, (ii) $c_p(A'^{(M)}) = 1$, (iii) if q is an odd prime dividing M , which is inert in $\mathbb{Q}(\sqrt{p})$, then $c_q(A'^{(M)}) = 2$, (iv) if q is an odd prime dividing M , which splits in $\mathbb{Q}(\sqrt{p})$, then $c_q(A'^{(M)}) = 4$.*

Proof. Assertion (i) follows immediately from the fact that $\mathbb{Q}(A'[2]) = \mathbb{Q}(\sqrt{p})$. The remaining assertions involving odd primes of bad reduction follow immediately from (4.11), on noting that $A'(\mathbb{Q}_q)[2]$ is of order 2 or 4, according as q does not or does split in $\mathbb{Q}(\sqrt{p})$, respectively. \square

4.2. Behaviour of Hecke eigenvalues. Recall that the L -function of an elliptic curve E over \mathbb{Q} is defined as an infinite Euler product

$$L(E, s) = \prod_{q \nmid C} (1 - a_q q^{-s} + q^{1-2s})^{-1} \prod_{q|C} (1 - a_q q^{-s})^{-1} =: \sum a_n n^{-s},$$

where

$$a_q = \begin{cases} q + 1 - \#E(\mathbb{F}_q) & \text{if } E \text{ has good reduction at } q, \\ 1 & \text{if } E \text{ has split multiplicative reduction at } q, \\ -1 & \text{if } E \text{ has non-split multiplicative reduction at } q, \\ 0 & \text{if } E \text{ has additive reduction at } q. \end{cases}$$

Here we give a result of the behaviour of the coefficients a_q of the L -function of elliptic curve A .

Theorem 4.9. *Let q be an odd prime distinct with the conductor p of A . Then we have that*

$$a_p = 1;$$

$$a_2 = \begin{cases} -1 & \text{if } p \equiv 1 \pmod{16}, \\ 1 & \text{if } p \equiv 9 \pmod{16}; \end{cases}$$

and

$$a_q \equiv \begin{cases} 2 \pmod{4} & \text{if } q \equiv 1 \pmod{4}, \\ 2 \pmod{4} & \text{if } q \equiv 3 \pmod{4} \text{ and } q \text{ is inert in } \mathbb{Q}(\sqrt{p}), \\ 0 \pmod{4} & \text{if } q \equiv 3 \pmod{4} \text{ and } q \text{ splits in } \mathbb{Q}(\sqrt{p}). \end{cases}$$

Proof. The assertion for a_p is clear as A has split multiplicative reduction at p .

For a_2 , we can do a straightforward calculation on the minimal form of A modulo 2, whence we get

$$y^2 + xy \equiv x^3 + \frac{u-1}{4}x^2 + 1 \pmod{2}.$$

When $u \equiv 1 \pmod{8}$, the above equation becomes $y^2 + xy \equiv x^3 + 1 \pmod{2}$, we then get $\#A(\mathbb{F}_2) = 4$, i.e. $a_2 = -1$. When $u \equiv 5 \pmod{8}$, the above equation becomes $y^2 + xy \equiv x^3 \pmod{2}$, we then get $\#A(\mathbb{F}_2) = 2$, i.e. $a_2 = 1$. The assertion then follows by noting $p = u^2 + 64$.

For a_q , first note that the 2-division field $\mathbb{Q}(A[2]) = \mathbb{Q}(i)$ and $\mathbb{Q}(A'[2]) = \mathbb{Q}(\sqrt{p})$, and we have the same L -function of A and A' . So we have that $A(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ when $q \equiv 1 \pmod{4}$, and $A'(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ when q splits in $\mathbb{Q}(\sqrt{p})$. Since $A(\mathbb{F}_q)[2]$ and $A'(\mathbb{F}_q)[2]$ are subgroups of $A(\mathbb{F}_q)$ and $A'(\mathbb{F}_q)$, respectively. We have that $4 \mid \#A(\mathbb{F}_q)$ and $4 \mid \#A'(\mathbb{F}_q)$. Then the assertions for $q \equiv 1 \pmod{4}$ and $q \equiv 3 \pmod{4}$ splitting in $\mathbb{Q}(\sqrt{p})$ follow by applying $a_q = q + 1 - \#A(\mathbb{F}_q)$. While for $q \equiv 3 \pmod{4}$ inert in $\mathbb{Q}(\sqrt{p})$, we have that $A(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z}$. It is easy to compute that $\mathbb{Q}(\sqrt{p})$ is a subfield of $\mathbb{Q}(A[4]^*)$, where $A[4]^*$ means any one of the 4-division points which is deduced from the non-trivial rational 2-torsion point of $A(\mathbb{Q})$. But q is inert in $\mathbb{Q}(\sqrt{p})$, that means $A(\mathbb{F}_q)[4] = A(\mathbb{F}_q)[2] \cong \mathbb{Z}/2\mathbb{Z}$. Hence $2 \mid \#A(\mathbb{F}_q)$, but $4 \nmid \#A(\mathbb{F}_q)$. Then the assertion follows in this case. This completes our proof. \square

4.3. 2-part of Birch and Swinnerton-Dyer conjecture. For the elliptic curve A , we have the following results.

Theorem 4.10. *We have*

$$\text{ord}_2(L^{\text{alg}}(A, 1)) = -1$$

for any prime p , with $p = u^2 + 64$ for some integer $u \equiv 5 \pmod{8}$.

For the Neumann-Setzer elliptic curves, Stein and Watkins [16] considered the parity of the modular degree of the map

$$\varphi : X_0(p) \rightarrow A.$$

They proved that $\deg(\varphi)$ is odd if and only if $u \equiv 5 \pmod{8}$. Next we shall prove Theorem 4.10. Before proving the theorem we first prove the following lemma.

Lemma 4.11. *For the modular parametrizations of A when $u \equiv 5 \pmod{8}$, $\varphi([0])$ is non-trivial, and is precisely the non-trivial torsion point of order 2.*

Proof. By the result of Stein and Watkins [16], the modular degree of A is odd if and only if $u \equiv 5 \pmod{8}$. Let $J_0(p)$ be the Jacobian of $X_0(p)$, and let B be the kernel of the map $J_0(p) \rightarrow A$. Denote C to be the cuspidal subgroup, which is known to be the torsion subgroup of $J_0(p)(\mathbb{Q})$, and it is generated by $[0] - [\infty]$ and cyclic of order n , where n is the numerator of $\frac{p-1}{12}$. We also have A is contained in $J_0(p)$ and $A(\mathbb{Q})[2] = C[2]$. We now assume that $\varphi([0])$ is trivial. Then C is contained in B . Thus the cardinality of the intersection of B and A is even. Then by [16, Lemma 2.2], the modular degree of A should be even, contradiction. Note that $A(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, thus $\varphi([0])$ is non-trivial, and is precisely the non-trivial 2-torsion point. \square

We now give the proof of Theorem 4.10.

Proof of Theorem 4.10. When $u \equiv 5 \pmod{8}$, we have $a_2 = 1$. Then by the modular symbol formula (2.1), we have

$$(1 + 2 - a_2)L(A, 1) = -\langle \{0, \frac{1}{2}\}, f \rangle.$$

Note that the point $[0]$ is equivalent to $[\frac{1}{2}]$ under $\Gamma_0(p)$, so $\langle \{0, \frac{1}{2}\}, f \rangle$ is an integral period (real) and in the period lattice Λ_f , i.e. $2 * \varphi([0]) \equiv 0 \pmod{\Lambda_f}$, as $\varphi([0]) = -I_f(0) = L(A, 1)$. Then by Lemma 4.11, $\varphi([0])$ is the non-trivial 2-torsion point, so the denominator of $\varphi([0])/\Omega^+$ must be 2, where Ω^+ is the least positive real period of A . Thus

$$\text{ord}_2(L^{\text{alg}}(A, 1)) = -1.$$

This completes the proof of Theorem 4.10.

A key point in the above proof is that the image of the cusp $[0]$ is the non-trivial 2-torsion point under the parametrization when $u \equiv 5 \pmod{8}$. After investigating many numerical examples we make the following conjecture.

Conjecture 4.12. *For any prime p , with $p = u^2 + 64$ for some integer $u \equiv 1 \pmod{4}$, we have*

$$\text{ord}_2(L^{\text{alg}}(A, 1)) = -1.$$

We now give the proof of Theorem 1.4.

Proof. Firstly, A is the $\Gamma_0(p)$ -optimal elliptic curve. By Theorem 4.9, we have $N_q \equiv 2 \pmod{4}$ when $q \equiv 2 \pmod{4}$ and is inert in $\mathbb{Q}(\sqrt{p})$. Secondly, note that when $u \equiv 5 \pmod{8}$, we have $\text{ord}_2(L^{\text{alg}}(A, 1)) = -1$ by Theorem 4.10. These satisfy the assumptions in Theorem 1.3, we then have $\text{ord}_2(L^{\text{alg}}(A^{(-q)}, 1)) = 0$. Naturally, $L(A^{(-q)}, s)$ does not vanish at $s = 1$. Both $A^{(-q)}(\mathbb{Q})$ and $\text{III}(A^{(-q)}(\mathbb{Q}))$ are finite by the theorem of Kolyvagin. The cardinality of $\text{III}(A^{(-q)}(\mathbb{Q}))$ is odd as $\text{III}(A^{(-q)}(\mathbb{Q}))[2]$ is trivial by Corollary 4.3. Then combining the results of Proposition 4.7, we know that the 2-part of Birch and Swinnerton-Dyer conjecture holds for $A^{(-q)}$. \square

We make the following proposition, which tells that the above result could be probably generalised to the twists of many prime factors. We denote $S''_m := \sum_{k=1}^m \chi(k) \langle \{0, \frac{k}{m}\}, f \rangle$.

Proposition 4.13. *Let $M = q_1 q_2 \cdots q_{2r}$, where r is any positive integer and q_1, q_2, \dots, q_{2r} are distinct primes congruent to 3 modulo 4 and inert in $\mathbb{Q}(\sqrt{p})$. Assuming Conjecture 4.12 and $\text{ord}_2(S''_M/\Omega^+) = \text{ord}_2(S'_M/\Omega^+)$, we then have that*

$$\text{ord}_2(L^{\text{alg}}(A^{(M)}, 1)) = 2r - 1,$$

for any integer $u \equiv 1 \pmod{4}$. Hence $L(A^{(M)}, s)$ does not vanish at $s = 1$, and so $A^{(M)}(\mathbb{Q})$ is finite, the Tate-Shafarevich group $\text{III}(A^{(M)}(\mathbb{Q}))$ is finite of odd cardinality, and the 2-part of Birch and Swinnerton-Dyer conjecture is valid for $A^{(M)}$.

The above proposition follows easily by Lemma 2.4, and combining the results given by Corollary 4.3 and Proposition 4.7.

Here we give some numerical examples supporting the above proposition. We take $p = 73$, i.e. $u = -3$, whence the elliptic curve A has a minimal Weierstrass equation given by

$$y^2 + xy = x^3 - x^2 + 4x - 3.$$

Moreover, $L^{\text{alg}}(A, 1) = \frac{1}{2}$ and it has discriminant -73^2 . Here are a list of primes which are congruent to 3 modulo 4 and inert in $\mathbb{Q}(\sqrt{73})$:

$$7, 11, 31, 43, 47, 59, 83, 103, 107, 131, 139, 151, 163, 167, 179, 191, 199, \dots$$

We take M to be the product of any two primes in the above list. We always have

$$\text{ord}_2(S''_M/\Omega^+) = \text{ord}_2(S'_M/\Omega^+) = 1.$$

It then follows that

$$\text{ord}_2(L^{\text{alg}}(A^{(M)}, 1)) = 1.$$

It is clear that the 2-part of Birch and Swinnerton-Dyer conjecture is valid for all of these twists of A .

REFERENCES

- [1] G. Boxer, P. Diao, *2-Selmer groups of quadratic twists of elliptic curves*, Proc. Amer. Math. Soc. 138 (2010), no. 6, 1969-1978.
- [2] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over \mathbb{Q} : wild 3-adic exercises*, J. Amer. Math. Soc. 14 (2001), no. 4, 843-939.
- [3] J. Coates, Y. Li, Y. Tian, S. Zhai, *Quadratic twists of elliptic curves*, to appear in Proc. Lond. Math. Soc..
- [4] J. Coates, *Lectures on the Birch-Swinnerton-Dyer conjecture*, Notices of the ICCM, 2013.
- [5] J. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, 1997.
- [6] J. Cremona, *Computing the degree of the modular parametrization of a modular elliptic curve*, Math. Comp. 64 (1995), no. 211, 1235-1250.
- [7] T. Dokchitser, V. Dokchitser, *On the Birch-Swinnerton-Dyer quotients modulo squares*, Ann. of Math. 172 (2010), 567-596.
- [8] V. G. Drinfeld, (1973), *Two theorems on modular curves*, (Russian) Funkcional. Anal. i Priložen. 7 (1973), no. 2, 83-84.
- [9] Ju. I. Manin, *Parabolic points and zeta-functions of modular curves*, Math. USSR-Izv. 6 (1972), 19-64.
- [10] J.-F. Mestre, J. Oesterlé, *Courbes de Weil semi-stables de discriminant une puissance m -ième*, (French) J. Reine Angew. Math. 400 (1989), 173-184.
- [11] O. Neumann, *Elliptische Kurven mit vorgeschriebenem Reduktionsverhalten. I*, (German) Math. Nachr. 49 (1971), 107-123.
- [12] O. Neumann, *Elliptische Kurven mit vorgeschriebenem Reduktionsverhalten. II*, (German) Math. Nachr. 56 (1973), 269-280.
- [13] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) 141 (1995), no. 3, 553-572.
- [14] B. Setzer, *Elliptic curves of prime conductor*, J. London Math. Soc. (2) 10 (1975), 367-378.
- [15] J. Silverman, *The arithmetic of elliptic curves*, Grad. Texts Math. 106, 1986, Springer.
- [16] W. Stein, M. Watkins, *Modular parametrizations of Neumann-Setzer elliptic curves*, Int. Math. Res. Notices (2004) no. 27, 1395-1405.
- [17] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) 141 (1995), no. 3, 443-551.
- [18] D. Zagier, *Modular parametrizations of elliptic curves*, Canad. Math. Bull. 28 (1985), no. 3, 372-384.

Shuai Zhai,
School of Mathematics, Shandong University,
Jinan, Shandong 250100, China, and
Department of Pure Mathematics and Mathematical Statistics,
University of Cambridge, UK.
shuaizhai@gmail.com